BRIAN J. STRETCH (CABN 163973)
United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JOHN H. HEMANN (CABN 165823)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7478
FAX: (415) 436-7234
john.hemann@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JING ZENG, Defendant.	Case No. CR 16-0172 JD UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS Date: November 9, 2016 Time: 10:30 am

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

FEDERAL RULES

OTHER AUTHORITIES

I. INTRODUCTION

This is not a case about an employee being prosecuted for deleting a file from his work computer. Nor is it a case about what defendant describes as "password sharing."

This is a case about an employee who was taking and misusing intellectual property that belonged to his employer. Acting for his own purposes, he invited outsiders to access company computers using his credentials. He mined a company database for valuable and confidential information that did not concern his employment duties. He stole documents regarding the company computer system and marketing plans. When he learned his employment was being terminated, he erased and reformatted his entire laptop computer for the purpose of concealing his misconduct from his employer.

The charges in the Superseding Information allege the criminal misuse of defendant's employer's computer facilities. Defendant's Rule 12(b) motion to dismiss should be denied for the simple and straightforward reason that the Superseding Information in which he is charged with two separate crimes arising from his conduct alleges the essential elements of those crimes, 18 U.S.C. §§ 1030(a)(5) (Count One) and 1030(a)(2)(C) (Counts Two and Three).

II. LEGAL STANDARD

Defendant's motion is governed by Fed. R. Crim. P. 12(b)(3)(B)(v). Defendant contends that the Information fails to state offenses under 18 U.S.C. §§ 1030(a)(5) and 1030(a)(2)(C). In asserting his position, defendant effectively ignores the legal standard under Rule 12 for measuring the sufficiency of a criminal charging document.

An information must contain "the statute, rule, regulation, or other provision of law that the defendant is alleged to have violated," and "a plain, concise, and definite written statement of the essential facts constituting the offense." Fed. R. Crim. P. 7(c)(1). Under Rule 12, sufficiency "is judged by whether the [information] adequately alleges the elements of the offense and fairly informs the defendant of the charge, not whether the Government can prove its case." *United States v. Blinder*, 10 F.3d 1468, 1471 (9th Cir. 1993) (citation and quotation marks omitted). The district court must "accept the truth of the allegations in the [information] in analyzing whether a cognizable offense has been

charged." *United States v. Boren*, 278 F.3d 911, 914 (9th Cir. 2002). An information "should be read in its entirety, construed according to common sense, and interpreted to include facts which are necessarily implied." *United States v. Hinton*, 222 F.3d 664, 672 (9th Cir. 2000).

Defendant suggests that the Court do exactly the opposite. He barely acknowledges the actual language of the Superseding Information and, when he does, suggests that the Court add elements to the plain language of the statute and interpret the alleged facts against the government.

III. FACTUAL BACKGROUND

Defendant Jing Zeng was an employee of Machine Zone, Inc., which makes the on-line video games Game of War: Fire Age, and Mobile Strike. He is charged in Count One with violating 18 U.S.C. § 1030(b)(5) by damaging his company computer without authorization by wiping and reformatting it after he used the computer to improperly accessed a database containing proprietary data and remove secret information from it. He also is charged in Counts Two and Three with violating 18 U.S.C. § 1030(a)(2)(C) by providing his company access credentials to unauthorized outsiders so that they could access company computers, along with instructions to assist them in accessing the computers.

///

Machine Zone hired Zeng in December 2014. In June 2015, defendant Zeng learned that his job at Machine Zone was not secure and that he would be forced to leave the company. The evidence will show that in July 2015, Zeng twice surreptitiously accessed a confidential company database called Tableau from his company laptop while not at work, and accessed files that contained valuable, non-public information regarding the way customers use and interact with the Machine Zone game. Zeng did this once before he was notified of his termination and once after. After he was terminated, Zeng "wiped" and reformatted his Machine Zone laptop before he returned it to the company, destroying key evidence regarding his access to the Tableau database. This conduct forms the basis for the computer damage charge alleged in Count One.

After the company reported the intrusion into Tableau to the FBI, the FBI learned that defendant's misconduct was part of a larger pattern. The FBI discovered Machine Zone trade secrets defendant should not have had in defendant's home during a search. The FBI also learned that

defendant had twice provided unauthorized access to Machine Zone's computer system to individuals in China who were not Machine Zone employees, the conduct which forms the basis for the unauthorized access charges in Counts Two and Three. The FBI's and Machine Zone's ability to further investigate this conduct was frustrated by the fact that defendant had wiped and reformatted his computer.

IV. ARGUMENT

A. The Factual Stipulation And Parties' Negotiations Are Irrelevant And Is Not Before The Court

Defendant begins by providing, at some length, background as to how the attorneys initially contemplated litigating the case. Discussions between the attorneys about proceeding by stipulation have been overtaken by events and are now neither factually nor legally relevant to the Court's decision on the pending motion.

To be sure, at one point the parties contemplated proceeding by asking the Court to focus entirely on the language of the original charging document, which mirrored a factual stipulation signed by the defendant. Two events changed that course. First, defendant filed a motion to dismiss that strayed considerably from the factual allegations in the original Information. Second, the Ninth Circuit decided *United States v. Nosal*, 828 F.3d 864 (9th Cir. 2016) ("*Nosal II*"), which, as defendant essentially concedes, permits the additional charges now contained in Counts Two and Three.

The original plan to proceed by stipulated facts has been overtaken by events and does not have continuing relevance.

B. The Decisions Of The Ninth Circuit Are Binding On This Court

A key premise of defendant's arguments is that two recent decisions of the Ninth Circuit were wrongly decided and should not be followed by this Court. Defendant contends that because the losing parties in those cases, *Nosal II* and *Facebook, Inc. v. Power Ventures, Inc.*, 828 F.3d 1068 (9th Cir. 2016), are seeking further review in the court of appeals, the decisions are not final and therefore are not binding on the district courts in the circuit.

This rather startling position is not supported by the cases defendant cites or any statute or rule of procedure. Defendant relies on cases in which the court of appeals wrote that it was not bound by its

own previous decisions under certain, limited circumstances. In *Natural Resources Defense Council, Inc. v. County of Los Angeles*, 725 F.3d 1194, 1203 (9th Cir. 2013), the court of appeals, on remand from the Supreme Court, stated that it was free to consider its earlier decision in the case in light of the Supreme Court's ruling. In *Carver v. Lehman*, 558 F.3d 869, 878 (9th Cir. 2008), the court of appeals held that it could amend a published opinion before it is final following the death of a panel member. Neither of these cases suggest that a district court is free to treat an opinion issued by a superior appellate court as anything other than binding.

An appellate decision becomes law – and therefore binding precedent as to the district courts – when it is issued. Circuit Advisory Committee Notes to Rule 35-3 state when rehearing en banc is granted, "[t]he three-judge panel opinion shall not be cited as precedent by or to this Court or any district court of the Ninth Circuit, except to the extent adopted by the en banc court." The negative implication is that until rehearing en banc is granted, the three-judge panel opinion is the law of the circuit. Every en banc grant contains that language. *In L.A. Branch NAACP v. L.A. Unified School District*, 750 F.2d 731, 736 (9th Cir. 1984) (en banc), the court stated, "We granted the NAACP's petition for rehearing en banc and withdrew the opinion of the three-judge panel." *See also Adebe v. Gonzalez*, 432 F.3d 1037, 1039 (9th Cir. 2005) ("we granted Petitioners' request for rehearing en banc, vacating the prior decision of the three-judge panel"). En banc review has not been granted in either *Nosal II* or *Power Ventures*, and therefore the decisions are binding as to the district courts in the Ninth Circuit.

C. Count One States A Violation Of 18 U.S.C. § 1030(a)(5)(A)

The Superseding Information charges the defendant with one count of violating 18 U.S.C. § 1030 (a)(5)(A). Defendant's motion to dismiss Count One should be denied because the Superseding Information alleges the elements of a violation of § 1030(a)(5)(A).

1. The Language Of The Statute

Section 1030(a)(5) criminalizes a variety of actions that cause computers to fail to operation as their owners intended. Subsection 1030(a)(5)(A), with which defendant is charged in Count One, provides that whoever "[k]nowingly causes the transmission of a program, information, code, or

command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; . . . shall be punished as provided in subsection (c) of this section."

Two statutorily-defined terms are relevant here. First, "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. §1030(e)(8). If damage results in "loss" of more than $5,000, then the violation of § 1030(a)(5)(A) is a felony. 18 U.S.C. § 1030(c)(4)(B)(i). Second, "[l]oss" means

> any reasonable cost to any victim, including the cost of responding to an offense, conduct a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. §1030 (e)(11).

2. Count One Allegations

In support of Count One, the Superseding Information (the "Information") alleges that, in November 2014, defendant was given a Mac laptop computer by his employer Machine Zone for the purpose of performing his job duties. Sup. Inf. ¶ 4. The Information alleges that this was a protected computer under 18 U.S.C. § 1030(a)(5)(A). *Id.* The laptop computer contained software installed by Machine Zone. *Id.*

Pursuant to company policy, which defendant received and acknowledged on November 26, 2014, when he received the computer, defendant was not permitted to "alter the equipment or change the use for which it was intended" and the software was not permitted to be "altered, copied, added or transferred at any time, unless authorized by a manager or the IT Department." Sup. Inf. ¶ 5.

In July 2015, defendant learned that his employment would be terminated by Machine Zone and knew that as a result he would be required to return his Mac laptop. Sup. Inf. ¶ 6.

According to the Information, before defendant returned the Mac laptop to Machine Zone, "through the transmission of computer codes and commands, Zeng damaged the Mac laptop by intentionally causing the contents of the Mac laptop to be erased, thereby altering and transferring the software on the computer." Sup. Inf. ¶ 7. The Information further alleges that defendant also "damaged the Mac laptop by reformatting it, installing on it an operating system other than that which was

installed by the company, and permanently removing certain items that had been installed originally by the company. He was not authorized by Machine Zone to do these things." *Id.*

Finally with regarding to Count One, the Information alleges that Machine Zone spent more than $5,000 for the services of computer forensic experts and others to investigate what had been deleted from the computer when defendant erased the contents. Sup. Inf. ¶ 8.

3. Count One States An Offense Under The Statute

The premise of defendant's argument has nothing to do with the essential question before the Court, which is whether the Superseding Information charges the elements of the statute. Defendant, instead, begins from the premise that the applicability of § 1030(a)(5)(A) to the present case is unclear because § 1030(a)(5)(A) "has not kept up with technology," a common theme promoted by defendants seeking to avoid the reach of the Computer Fraud and Abuse Act (hereafter "the CFAA").

The defendant also argues that he did not violate the CFAA which was intended to combat "hacking," a term which is not defined by statute. Indeed, "hacking" has no legal meaning separate from the provisions of the CFAA. *See e.g. Vanderhye v. IParadigms*, 562 F.3d 630, 645 (4th Cir. 2009). For example, the defendant asserts that the purpose of the CFAA's damage provisions are solely to "target conduct that denies privileges to other users, such as sending out computer viruses and launching denial-of-service attacks," paradigmatic examples of "hacking." However, both the plain meaning of the statute's language and the legislative history of the CFAA's damage provisions contemplate a broader scope. The legislative history is clear that the CFAA's damage provisions apply to "insiders," persons who have some authorization to access a computer, and who intentionally cause damage to the computer. See S. REP. 104-357, 11 ("in sum, under the [1996 amendments] bill, *insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer*, not for recklessly or negligently causing damage. By contrast, *outside* hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass") (emphasis added); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1127 (WD. Wash. 2000) ("[t]he defendant also maintains the CFAA is limited to "outsiders" or "hackers," and not "insiders" (employees)).

///

Though the original scope of the CFAA was limited to the concerns addressed by the defendant, its subsequent amendments have broadened the scope sufficiently to cover the behavior alleged in this case"). Furthermore, the plain language of § 1030(a)(5)(A) extends its reach to intentional conduct without authorization which results in "*any* impairment to the integrity or availability of data, a program, a system, or information." Reformatting a hard drive, and re-installing some system software, but not any data on the system, is "damage" because it is an "impairment to the integrity and availability" of the computer.

Defendant asserts that the Information's allegations are defective because the (a) defendant's conduct is merely an "exceed authorization" violation of a corporate computer use restriction which is not criminal under the Ninth Circuit's decision in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) ("*Nosal I")*; (b) the "transmission" allegations are not sufficient; (c) "mere" deletion of computer files is not "damage"; and (d) section 1030(a)(5) requires "permanent" deletion of data which renders the data unrecoverable.

(a) The Defendant Was Not Authorized To Reformat The Computer's Hard Drive

This is not a *Nosal I* case. In *Nosal I,* the court of appeals dealt with a situation in which the defendant was authorized to access a computer system. Here, the defendant was not authorized to damage his computer the way he did.

The Superseding Information alleges that the defendant was not authorized *at all* to re-format the computer's hard drive and delete all data. As such, this is *not* a case which relies on the CFAA's definition of "exceeding authorized access." In *Nosal I,* the 9th Circuit addressed the meaning of the term "exceeds authorized access" in 18 U.S.C. § 1030(e)(6) in a case where a defendant had permission to access information on a computer, but did so for a purpose not condoned by a user agreement. The court held that the CFAA's definition of "exceeds authorized access" is limited to violations of restrictions on access to information, and does not apply restrictions on the use of that information. 676 F.3d at 863-64. However, as noted on remand to the district court, the 9th Circuit expressly did not address limits the manner in which authorization can be limited. *United States v. Nosal*, 930 F. Supp. 2d 1051, 1060 (ND. Cal. 2013). The holding in *Nosal* does not address criminal liability where a defendant

expressly did not have authorization to undertake certain action on a computer which belongs to his employer.

Subsequently in *Nosal II*, the Ninth Circuit considered the plain and ordinary meaning of the words "without authorization." Concluding that the term is not ambiguous, the *Nosal II* court held that "authorization" means "permission or power granted by an authority," or "official permission to do something; sanction or warrant." The court noted that implicit in the definition of authorization "is the notion that someone, including an entity, can grant or revoke that permission," in that case the owner of a computer database. In this case, the defendant is alleged to have reformatted, or deleted, the entire contents of the hard drive of his company-issued laptop. He later re-installed only some of the software which was originally on the machine. However, Machine Zone, Inc. expressly prohibited the defendant from "alter[ing] the equipment or change the use for which it was intended." Moreover, software installed on the computer was not permitted to be "altered, copied, added or transferred at any time, unless authorized by a manager or the IT Department." Rather than a case where the defendant is alleged to have exceeded his authorized access, this is a case where the defendant had no permission at all to reformat the computer, and in so doing, he intentionally caused damage without authorization.

An employer may restrict an employee's authorization to alter the software configuration of a computer, or to reformat a computer. In *Clarity Services v. Barney*, 698 F.Supp.2d 1309 (MD Fla. 2010), the defendant employee had resigned his employment. The defendant was purported worried that "sensitive" consumer data might remain on the laptop when it was shipped to his employer. To prevent the employer from "suffer[ing] any exposure if [the computer] was lost in transit," the defendant "reset" the laptop before returning the computer to his employer. *Id.* at 1313. The court noted that the defendant testified that a user "resets" a laptop by booting the computer, pressing one of the function keys during startup, and selecting an option to restore the computer back to factory state. Resetting the computer permanently deleted all information stored on the computer and re-installed the operating system. As a result, forensic examination of the computer could not recover any deleted data because the hard drives "had been zeroed out, which is a term in the computer industry for a drive that had been—zeros had written to the blank sectors so that no data on the drive could be recovered." *Id.* at 1316. In *Clarity Services*, the employer did not impose any restriction on the defendant's use of the computer, including

reformatting the hard drive. Because the defendant "enjoyed unrestricted access to all of the information on the laptop throughout his employment," and could read, modify, or delete any file, the court concluded that the defendant neither accessed the laptop "without authorization" nor "exceeded his authorized access" to the laptop when he reformatted the laptop's hard drive. *Ibid.*

In this case, Machine Zone's policy restricted the defendant's authorization to alter the installed software, or reformat the laptop's hard drive[1], which cause the irretrievable loss of any data that was on the laptop when the hard drive was wiped.

For example, in *Keen v. Bovie Medical Corp*, 2013 WL 1899791 (MD Fla. May 7, 2013), the court held that the plaintiff's intentional wiping of a hard drive resulting in data loss was sufficient to state a claim under §1030(a)(5)(A). In *Keen*, the defendant Bovie Medical Corp. filed a counterclaim against the Plaintiff Keen alleging damage without authorization to a company laptop used by Keen. Keen had used a program to wipe the laptop clean and no data was recoverable. The *Keen* court held that wiping a laptop's hard drive amount to the permanent deletion of data which constitutes damage under §1030(a)(5)(A).

Similarly, in *B & B Microscopes v. Armogida*, 532 F.Supp.2d 744 (WD Pa. 2007), the court held that the defendant violated §1030(a)(5)(A) when the defendant knowingly and intentionally deleted files on the laptop, including records of sales, service, customer lists, and other business matters, all in violation of his employer's restriction against removing the employer's files. Indeed, the defendant in *B & B Microscopes* selectively deleted files, which the defense in this case derides as "mere" deletion, and did not re-format the entire hard drive.

(b) By Reformatting The Laptop Hard Drive And Installing New Software, The Defendant Knowingly Transmitted A Code Or Command Which Impaired "The Integrity Or Availability Of Data, A Program, A System, Or Information"

[1] Defendant also argues, without citation, that given his "high-ranking" position in the company, he could authorize himself to alter the computer by deleting all of the data on the computer. Contrary to defendant's assertion, mere possession of his employer's computer does not make him an "account holder" or give him any greater authorization to the computer than the restrictions placed on him by the owner of the device, which is his employer. In any event, the Information alleges that he did not have authorization and at this point in the case, that is all that matters.

Defendant argues further that there was no "transmission" of a command or code as required by §1030 (a)(5)(A), and requires permanent loss of data in this case. Defendant cites to several cases which involve the theft of proprietary information, ostensibly for the proposition that §1030 (a)(5)(A) requires "permanent loss of data." For example, in *Custom Packaging Supply, Inc. v. Phillips*, 2016 WL 1532220 (E.D. Cal April 15, 2016), which the defendant claims is directly on point to the issues in this case, the plaintiff sued the defendants for misappropriation of trade secrets. The plaintiff alleged that the defendants had downloaded information regarding proprietary designs, customer data and other confidential information to compile an "illegal library" which they passed on to a competitor. *Phillips*, 2016 WL 1532220 at *1. Because the plaintiff's alleged only that the defendants removed the plaintiff's files from its servers, and did not allege that the defendants damaged systems or destroyed data, the court dismissed the plaintiff's 1030 (a)(5) claim. *Id.* at *4.

Similarly, in *Condux Intern. V. Haugum*, 2008 WL 5244818 (D. Minn. Dec. 15, 2008), the plaintiff alleged that the defendant misappropriated confidential business information to start a competing business. The court dismissed the plaintiff's claim because the complaint alleged only a compromise of diminishment of the confidentiality, exclusivity, or secrecy of the proprietary information, and 1030 (a)(5) requires "some alteration of or diminution to the integrity, stability, or accessibility of the computer data itself." *Condux Intern.* at *8 ("the complained of activity must have an effect on the binary coding used to create, store, and access computerized representations of information"). *Condux Intern.* did not hold that §1030 (a)(5) requires "permanent deletion" of data.

Defendant also cites *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla. Aug 1, 2006), another case concerning alleged trade secret theft. The court noted that allegedly stealing trade secrets is not "damage" within the meaning of §1030 (a)(5). Plaintiff urged that the court infer from the pleadings that the defendants had also permanently deleted the stolen data from Lockheed Martin's servers, which the court refused to do noting that "in the absence of an allegation of permanent deletion or removal, the Court will not create one." *Speed* did not hold that §1030 (a)(5) requires permanent deletion of data.

Even if this court concludes that 1030(a)(5)(A) requires a permanent deletion of data which is not available through other means, it is a fair inference that data stored on the defendant's laptop, and

nowhere else, is not available through other means when the defendant reformatted the laptop's hard drive without authorization. In *Cheney v. IPD Analytics, LLC*, 2009 WL 1298405 (SD Fla April 16, 2009), the plaintiff alleged that the defendant destroyed thousands of computer files on the plaintiff's computers to conceal the defendant's "disloyal actions." The district court rejected a civil claim under 1030 (a)(5), holding that deletion of files alone does not constitute damage under 1030(a)(5) if the deleted data is still available to the plaintiff through other means. Here, however, all of the data files stored on the defendant's computer were lost permanently when the defendant reformatted the laptop's hard drive.

Similarly, reformatting a hard drive satisfies the requirement that the defendant knowingly caused a transmission which intentionally caused damage without authorization. In *International Airport Centers, LLC v. Citrin*, 440 F. 3d 419 (7th Cir. 2006), the court interpreted the word "transmission" in 1030 (a)(5). Although the defendant interprets *Citrin* to mean that pressing the delete button is not a "transmission," Judge Posner's opinion for the court simply illustrates a more sophisticated understanding of how computer files are deleted. According to *Citrin*, pressing the "delete" key on a computer ordinarily does not actually delete anything:

> pressing the "delete" key on a computer (or using a mouse click to delete) does not affect the data sought to be deleted; it merely removes the index entry and pointers to the data file so that the file appears no longer to be there, and the space allocated to that file is made available for future write commands. Such deleted files are easily recoverable.

Citrin, id. at 419.

Pressing a delete key is insufficient because pressing a delete key actually does not delete a digital file from the computer. By analogy, clearing a web browser cache, or deleting a personal email, similarly does not delete the digital file from the computer and these files are usually recoverable from a hard drive. However, the defendant in *Citrin* did more than "merely" delete – he loaded into the laptop a secure-erasure program designed to overwrite the deleted files and to prevent their recovery. The court noted that the precise mode of transmission did not much matter, especially with Congress' concern with "two types of attack: attacks by virus and worm writers, on the one hand, which come from outside, and attacks by disgruntled programmers who decide to trash the employer's data system

on the way out…." *Id.* at 420. The latter is defendant Zeng, an employee who trashed his employer's property on the way out.

Similarly, in *KLA-Tencor Corp. v. Murphy*, 717 F.Supp.2d 895, 903 (N.D. Cal. 2010), the court considered a case similar to this in which an employee deleted confidential information from his company computer. Judge Whyte held that "the loading of a program onto a computer, whether by disk or internet download, constitutes a 'transmission' under 18 U.S.C. § 1030(a)(5)(A)(i)." The Information in this case alleges that, as part of his course of conduct to delete and reformat his computer, defendant Zeng loaded new software onto his computer.

(c) The Information Adequately Alleges That The Defendant Intended To Cause Damage

The defendant also argues that despite the allegation in the Criminal Information that the defendant intended to cause damage to the computer, the defendant could have accidentally caused damage to Machine Zone's computer.

The Information alleges that defendant intended to cause damage. That alone is enough at the pleading stage. Moreover, taking the additional allegations in the light most favorable to the government, the allegations are sufficient to establish that by reformatting the hard drive, the natural and proximate result of his conduct was to impair the integrity of the software and data on the computer. The law does not require the government to allege in the charging document the specific files that were permanently deleted or newly installed on defendant's computer, as he suggests is necessary.

The hypotheticals defendant spins are not helpful to his cause. This is not like installing an Apple update; defendant erased his entire computer and reinstalled a new operating system immediately before he was required to return his computer to the company.

(d) The Information Adequately Alleges Loss Over $5,000

Defendant argues that the allegation of loss is insufficient because the costs of responding to defendant's conduct may not have been reasonably necessary. First, the allegations of the Criminal Information tracks the language of the statute, which requires loss of more than $5,000 to allege a felony violation of 1030 (a)(5)(A). This is sufficient under the standard applicable to motions to dismiss. Second, "loss" is a broad concept which covers costs associated with investigating an incident. *See*

Animators at Law, Inc. v. Capital Legal Solutions, LLC, 786 F. Supp. 2d 1114 (ED Va. 2011); *KLA-Tencor*, 717 F.Supp.2d at 903; *iParadigms*, *supra*. The statutory definition of "loss" includes "any reasonable cost to any victim, including the cost of responding to an offense." 18 U.S.C. § 1030(e)(11). Investigative costs such as forensic examination expenses to determine what data was deleted, and whether any of it is recoverable, are appropriate elements of loss and is properly alleged in the Information.

D. Counts Two And Three State Violations Of 18 U.S.C. § 1030(A)(2)(C)

Defendant moves to dismiss Counts Two and Three, which allege violations of 18 U.S.C. § 1030(a)(2)(C) arising from defendant's sharing of his Machine Zone access credentials with third parties and providing instructions for them to use those credentials to access Machine Zone computers. In his motion, defendant essentially concedes that *Nosal II* decides the issue before the Court. As noted above, the Court bound to follow this decision and, accordingly, defendant's motion to dismiss these counts should be denied.

1. Language of the Statute

Section 1030(a)(2)(C) provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" is guilty of violating the CFAA. 18 U.S.C. § 1030(a)(2)(C). The offense is punished as a misdemeanor when, as here, additional elements are not alleged and proven. 18 U.S.C. § 1030(c)(2)(A).

As will be discussed below, elements such as "knowingly," "mantle of authority," and "revocation" are neither required under the plain language of the statute or held by decisional law to be elements of the offense.

2. Allegations in Support of Counts Two and Three

Counts Two and Three of the Information allege that defendant aided and abetted unauthorized access to Machine Zone's protected computer system, in violation of § 1030(a)(2)(C). Specifically, both counts allege that defendant "intentionally accessed a computer without authorization and exceeded authorization, and thereby obtained information from a protected computer." Sup. Inf. ¶ ¶ 10 & 13. This charging language tracks the statutory language.

The Superseding Information alleges that defendant "directed and caused" outsiders who were not employees "of Machine Zone to access a restricted and confidential Machine Zone computer system and domain using Zeng's company-issued access information." Sup. Inf. ¶¶ 11 & 14. The Information alleges that defendant "instructed and advised" the outsiders "to download and install a beta version of a newly developed and unreleased mobile video game and to test the game from within China" on mobile phones. *Id.* Defendant provided the outsiders "with information and instructions on how to access information within the computers." *Id.*

Both Count Two and Count Three are charged as misdemeanors.

3. Counts Two and Three State Offenses Under § 1030(a)(2)(C)

Counts Two and Three allege, tracking the language of the statute, that defendant Zeng intentionally provided his access credentials to outsiders and then directed them as to how to access Machine Zone's computer system.

Defendant acknowledges that the Ninth Circuit's decision in *Nosal II* supports the charges, but pokes and prods at various places in an attempt to find a soft spot to exploit. His attempts are not persuasive.

This is primarily so because *Nosal II* is relevant only to one element of the charges in Counts Two and Three, the "without authorization" element. *Nosal II* involved charges under section 1030(a)(4), not section 1030(a)(2) which is charged in this case. The "without authorization" language is common to both (a)(4) and (a)(2), and the *Nosal II* court's interpretation of that language supports the charges alleged here. In important other respects, particularly defendant's argument regarding the statutory mens rea, the language of sections (a)(4) and (a)(2) are different and defendant's argument, therefore, fails.

(a) The Information properly alleges that defendant aided and abetted outsiders without authorization to access Machine Zone's computer system.

The Superseding Information alleges that defendant provided company outsiders – individuals "without authorization" – with his access credentials and then instructed them how to use those credentials to enter the Machine Zone computer system, which they did. The Information alleges this conduct to be intentional, as the statute requires.

In the *Nosal* cases, the defendant was a former employee of an executive search firm. Before he left the firm, he accessed the firm's computer system, took confidential information, then used that information after his departure in his new job. In *Nosal I*, the court of appeals held that did not "exceed authorized access" because while still an employee Nosal in fact had access to the computer system from which he took the information. However, after Nosal left the firm, he used a remaining employee's access credentials to again access the computer systems. Now an outsider, the court of appeals held in *Nosal II*, Nosal no longer possessed authorized access to the computer system and thus acted "without authorization."

The "without authorization" language of the statute is "straightforward" as applied to outsiders. *Nosal II*, 828 F.3d at 873. It applies, the court of appeals made clear, to "outside hackers" who do not have authority to access computer systems, as opposed to "inside hackers" who do have such authority. *Id.*at 874. In *Nosal II*, the court of appeals upheld the conviction of outsiders (former employees) who used an insider's access credentials to access the company's computer system because the outsiders acted "without authorization."

This, of course, is why defendant concedes that *Nosal II* makes his argument to dismiss "more complicated," Def. Mem. at 7:21, and urges the Court to simply disregard it – which the Court is not permitted to do. The Superseding Information alleges that defendant provided his access credentials to an outsider for the purpose of allowing the outsider to access the company's computer system.

(b) "Revocation" and "mantle of authority" allegations are not elements of the offense and are not required to be alleged

Defendant contends that, if the Court determines that it must follow *Nosal II*, that the government was required to allege additional elements that were present in the *Nosal II* case.

First, he contends that *Nosal II* requires proof that the outsider's access credentials were revoked. This argument is meritless. In *Nosal II*, the issue of revocation of access credentials was relevant only because Nosal was once an employee (insider) and once had access to the computer system. The crimes affirmed by the court of appeals occurred after he left, became an outsider, and lost the authorization he once had. It was the revocation of Nosal's access credentials, concomitant with him leaving the company, that transformed him from an insider to an outsider.

Here, the Superseding Information simply alleges that the unauthorized computer access was performed by "outsiders" in China. There was no revocation because the outsiders in this case, unlike Nosal, never had authorized access in the first place. To accept defendant's revocation argument would mean that only former employees whose computer access was revoked could be prosecuted under the "without authorization" provisions CFAA, outsiders who never had such access could not be prosecuted because their authorization could not be revoked.

Second, defendant contends that the Superseding Information is defective because it does not allege a negative – that the outsiders lacked a "mantle of authority" derived from defendant when they accessed the Machine Zone computer system. This argument is simply another way of articulating the first argument, that a "revocation" of a "mantle of authority" is a necessary element of the offense. "Mantle of authority" is not an element of the statute and thus need not be plead. If, as a factual matter, the outsiders were actually authorized to access the company computers, that might be a defense at trial, but it is not required to be alleged in the Information.

(c) "Knowingly" is not the mens rea prescribed by Congress

Defendant argues that the Superseding Information fatally fails to allege that the defendant or the outsiders acted "knowingly." Defendant cites language from the decisions in *Power Ventures* and the oral argument in *Nosal II* in support of his argument. Neither case, however, addresses or the issue of whether an Information alleging a violation of 18 U.S.C. § 1030(a)(2)(C) must specifically allege "knowingly" as the mens rea.

The statute charged here does not use the word "knowingly," and instead uses "intentionally" as the required mens rea. 18 U.S.C. § 1030(a)(2)(C). This was purposeful. In 1986, Congress changed the intent standard in this section from "knowingly" to "intentionally" in order to emphasize that "intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe." S. Rep. No. 432, 99th Cong., 2d Sess., *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483. It also designed the "'intentional' standard to focus federal criminal prosecutions on those whose conduct evinces a clear *intent to enter*, without proper authorization, *computer files or data belonging to another*." *Id.* at 2484 (emphasis added); *see also United States v. Willis*, 476 F.3d 1121, 1125 n.1 (10th Cir. 2007). In this respect, § 1030(a)(2) offenses are analogous to

traditional theft offenses in which the question is whether the defendant intended to steal something that does not belong to him. "Knowingly" is not a necessary in these kinds of cases. See, *e.g.*, *United States v. Derrington*, 229 F.3d 1243 (9th Cir. 2000).

Defendant's reliance on *Power Ventures* and *Nosal II* is misplaced. *Nosal II* involved violations of 18 U.S.C. § 1030(a)(4), which, unlike § 1030(a)(2)(C), expressly includes "knowingly" as an element of the offense. Defendant's reliance on *Power Ventures*, also is improper because the case did not address let alone casually hold that "knowingly" is an element of a § 1030(a)(2)(C) violation, which would have been contrary to Congressional intent. The language cited from *Power Ventures* is at most dictum, but is more likely just the court's passing characterization of the evidence relevant to the issue of unauthorized access on which it was focused.

The Superseding Information faithfully tracks the language of the charged statute and fully, directly, and expressly sets forth all the elements necessary to constitute the offense intended to be proved. It is therefore sufficient. *See Hamling v. United States*, 418 U.S. 87, 117–18 (1974); *United States v. Tavelman*, 650 F.2d 1133, 1137 (9th Cir.1981). An indictment that follows the statutory language, and otherwise puts the accused on fair notice of all the implied elements of the charge, is sufficient without including all judicial interpretations of the words used in the statute. *See United States v. Godinez–Rabadan*, 289 F.3d 630, 634 (9th Cir. 2002); *see also United States v. Renteria*, 557 F.3d 1003, 1006 (9th Cir. 2009) (discussing previous opinion that rejected argument that indictment must include allegations that are merely "judicial gloss" upon the statutory language).

(d) The Information sufficiently alleges the outsider's liability

The Superseding Information alleges that defendant is liable as an aider and abettor for providing his access credentials to outsiders who, without authorization, accessed Machine Zone's computer system. In challenging this, defendant essentially repeats all of this previous arguments and directs them not to himself, but to the outsiders he aided, abetted, and willfully caused to access the Machine Zone computers without authorization.

Defendant again contends that the Information is flawed because *Nosal I* prohibits prosecutions based on "password sharing" and *Nosal II* and *Power Ventures* are not good law. Def. Mem. at 11. He further argues that to prove the liability of the outsiders (aided and abetted by defendant Zeng), the

government must allege and prove both "revocation" and "knowing" conduct under *Nosal II* and *Power Ventures*. Def. Mem. at 11. All of these arguments should be rejected for the reasons set forth above. *Nosal II* and *Power Ventures* are binding and must be followed. Neither "knowingly" nor "revocation" are elements of the offense alleged in the Information and they need not be alleged against the outsiders any more than they do against defendant as the aider and abettor.

V. CONCLUSION

Defendant's motion to dismiss should be denied.

DATED: October 20, 2016

Respectfully submitted,

BRIAN J. STRETCH
United States Attorney

John H. Hemann

JOHN H. HEMANN
Assistant United States Attorney